UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA,	§	CRIMINAL NO.:
	§	
Plaintiff,	§	**INFORMATION**
v.	§	
	§	**Ct. 1**: 18 U.S.C. § 371
ANDREW PERCY TRUJILLO (1),	§	Conspiracy to Commit
	§	Computer Fraud and Abuse
ZENA ELISA DOUNSON (2),	§	and Wire Fraud
	§	
Defendants.	§	**5:22-CR-451-JKP**

THE UNITED STATES ATTORNEY CHARGES:

INTRODUCTION

At all times relevant to this Information:

PERSONS AND ENTITIES

1. Defendant **ANDREW PERCY TRUJILLO (1)** resided in Bexar County, within the Western District of Texas.

2. Defendant **ZENA ELISA DOUNSON (2)** resided and did business in Bexar County, within the Western District of Texas.

3. Victim 1 was a resident of the State of California.

4. Victim 2 was a resident of the State of West Virginia.

TECHNICAL TERMS

5. A "SIM" card is an acronym for a Subscriber Identity Module card, which is a chip located inside a cell phone that stores information identifying and authenticating a cell phone subscriber. When a cell phone carrier reassigns a phone number from one physical phone to another—such as when a customer purchases a new phone but wants to retain the same number—the carrier switches the assignment of the cell phone number from the SIM card in the old phone

to the SIM card in the new phone. This process is sometimes called "porting" a number. "SIM swapping" is a term for essentially the same process conducted without the authorization of the individual who legitimately controls the number.

6. Cybercriminals generally engage in SIM swapping by convincing a victim's cell phone carrier to reassign the victim's cell phone number from the SIM card inside the victim's cell phone to the SIM card inside a cell phone controlled by the cybercriminals. For instance, the cybercriminal may pose as the victim and claim his cell phone was lost or damaged, and that he needs to have his number transferred to another phone. Alternatively, the cybercriminal may claim to be a representative of the carrier working at a local store, with a customer who needs to have their number ported to a new device.

7. An "account takeover" is a technique that cybercriminals use to take control of a victim's online accounts (e.g., a victim's email, social media, or cryptocurrency accounts) without authorization. Cybercriminals use a variety of techniques to conduct account takeovers. For example, cybercriminals who successfully SIM swap a victim may then pose as the victim with an online account provider and request that the provider send account password-reset links or an authentication code to the SIM-swapped device now controlled by the cybercriminals. The cybercriminals can then reset the victim's account log-in credentials (*e.g.*, username and password), even if the victim has tried to secure the account by requiring that an authentication code be sent ("two-factor authentication"). Cybercriminals can then use the log-in credentials to access the victim's account without authorization, (*i.e.*, "hack into" the account).

8. In a SIM swapping scheme, one or more individuals play the role of the "holder." A holder physically holds the SIM card and provides the SIM card number to a co-conspirator with access to the phone carrier's systems. After the phone number is swapped, the holder receives

the victim's phone calls and text messages. A holder could then complete the account takeover process and access the victim's accounts or pass the victim's credentials to another co-conspirator.

9. Cryptocurrency is an umbrella term for a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, generally with relative anonymity. Popular examples of cryptocurrencies include Bitcoin and Ethereum. Users maintain "wallets" and maintain online accounts with cryptocurrency exchanges such as Coinbase, Poloniex and Block.io.

10. Cybercriminals who engage in SIM swapping, account takeovers, and cryptocurrency theft often collaborate with one another online, using various online monikers, in underground forums such as "Discord," "OGUsers" and "Hackforums," as well as using real-time communications platforms.

COUNT ONE
Conspiracy to Commit Computer Fraud and Abuse and Wire Fraud
[18 U.S.C. § 371]

11. Paragraphs 1-10 are realleged and incorporated by reference.

12. From on or about November 18, 2021, to on or about November 26, 2021, in the Western District of Texas, and elsewhere, the Defendants,

ANDREW PERCY TRUJILLO (1)
and
ZENA ELISA DOUNSON (2),

along with others known and unknown to the United States Attorney, conspired with each other to commit the following offenses:

a. Computer fraud and abuse, that is, intentionally accessing a protected computer without authorization and thereby obtaining information, in furtherance of any criminal and tortious act in violation of the laws of the United States, specifically wire fraud, in violation of Title 18, United States Code, Section 1343, all in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(ii).

b. Computer fraud and abuse, that is, knowingly causing the transmission of a program, information, code, and command, and as a result of such conduct, intentionally causing damage without authorization to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A); and

c. Wire fraud, that is, having devised and intending to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, transmitting and causing to be transmitted, by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures and sounds, for the purpose of executing the scheme to defraud, in violation of Title 18, United States Code, Section 1343.

Objects and Purpose of the Conspiracy

13. It was the object of the conspiracy and the scheme and artifice to defraud to unlawfully enrich **ANDREW PERCY TRUJILLO (1)**, **ZENA ELISA DOUNSON (2)**, and others known and unknown to the United States Attorney, by fraudulently gaining unauthorized access to the computer networks of wireless and other electronic account providers and using that unauthorized access to take control of victims' electronic and financial accounts and steal amounts of digital currency. The purpose of the conspiracy was to obtain things of value from the victims, including, but not limited to, cryptocurrency and control of the victims' online accounts with cryptocurrency exchanges.

Manner and Means of the Conspiracy

14. Among the manner and means by which **ANDREW PERCY TRUJILLO (1)**, **ZENA ELISA DOUNSON (2)**, and others known and unknown to the United States Attorney carried out the conspiracy were the following:

a. Identifying potential victims who likely had significant amounts of cryptocurrency.

b. Researching the potential victims using online tools.

c. Engaging in "SIM swapping" in order to take control of victims' cell phone numbers.

d. Leveraging their control over victims' cell phones to obtain unauthorized access to the victims' online accounts, including email accounts, social media accounts, and cryptocurrency accounts.

e. Using their access to victims' accounts, to take control of, and steal things of value from the victims' online accounts, including their account handles and their cryptocurrency.

f. Selling or otherwise transferring victims' log-in credentials, account handles, and cryptocurrency to others in exchange for money or other things of value.

g. Communicating with co-conspirators via online social media and chat platforms.

h. Using multiple online accounts to hide their identities and evade detection by law enforcement.

Overt Acts in Furtherance of the Conspiracy

15. On or about November 18, 2021, the cell phone number of Victim 1 was swapped to a phone controlled by TRUJILLO. TRUJILLO was the holder for this SIM swap. Utilizing SIM card information provided by DOUNSON, TRUJILLO and DOUNSON caused text messages containing two-factor authentication codes for Victim 1's Cryptocurrency Exchange A account to be sent to the cell phone controlled by TRUJILLO.

16. On or about November 18, 2021, TRUJILLO, DOUNSON, and other co-conspirators performed an account takeover of Victim 1's computer network, taking control of wireless calls and text messages sent to the accounts of Victim 1. TRUJILLO then accessed Victim 1's Cryptocurrency Exchange A account and transferred Ethereum valued at the time at approximately $47,123.00 at the time to one or more cryptocurrency wallets controlled by TRUJILLO and his co-conspirators.

17. On or about November 26, 2021, the cell phone number of Victim 2 was swapped to a phone controlled by TRUJILLO. TRUJILLO was the holder for this SIM swap. Utilizing SIM card information provided by DOUNSON, TRUJILLO and DOUNSON caused text messages

containing two-factor authentication codes for Victim 2's Cryptocurrency Exchange B account to be sent to the cell phone controlled by TRUJILLO.

18. On or about November 26, 2021, TRUJILLO, DOUNSON, and other co-conspirators performed an account takeover of Victim 2's computer network, taking control of wireless calls and text messages sent to the accounts of Victim 2. TRUJILLO, DOUNSON, and other co-conspirators performed an account takeover and accessed Victim 2's Cryptocurrency Exchange B account and transferred Ethereum valued at the time at approximately $235,201.00 at the time to one or more cryptocurrency wallets controlled by TRUJILLO and his co-conspirators.

All in violation of Title 18, United States Code, Section 371.

ASHLEY C. HOFF
UNITED STATES ATTORNEY

BY: _____
For Matthew W. Kinskey
Assistant United States Attorney

For _____
Michael C. Galdo
Assistant United States Attorney